

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1-3. (Canceled)

4. (Currently Amended) [[A]] The terminal according to claim 22, wherein the key for the encrypted cryptographic algorithm is a key for secret key cryptography.

5. (Currently Amended) [[A]] The terminal according to claim 22, wherein the key for the encrypted cryptographic algorithm is a key for public key cryptography.

6. (Canceled)

7. (Currently Amended) [[A]] The terminal according to claim 22, wherein said control ~~means~~ section instructs said cryptographic algorithm storage section to output a requested cryptographic algorithm upon receiving a transmission request for any one of the cryptographic algorithms stored in said cryptographic algorithm storage section, and

said encryption/decryption ~~means~~ section encrypts the requested cryptographic algorithm as the information to be transmitted.

8. (Currently Amended) [[A]] The terminal according to claim 22, wherein when a partner with which said terminal communicates is an apparatus including said cryptographic communication terminal, said terminal:

requests the partner for a new cryptographic algorithm and/or a key for a corresponding encrypted algorithm~~[[,]]~~;

decrypts a corresponding response by using said encryption/decryption ~~means~~ section~~[[,]]~~;

stores the requested cryptographic algorithm in said cryptographic algorithm storage section upon receiving the cryptographic algorithm~~[[,]]~~; and

stores the requested key for the encrypt algorithm in said key information storage section upon receiving the key.

9. (Currently Amended) A cryptographic communication center apparatus comprising said cryptographic communication terminal defined in claim 22, wherein when the algorithm decryption key is requested from the partner, said apparatus inputs the corresponding algorithm decryption key as the information to be transmitted to the partner to said encryption/decryption ~~means~~ section.

10. (Currently Amended) [[An]] The apparatus according to claim 9, wherein: said apparatus comprises said cryptographic communication terminal~~[[,]]~~ and an update cryptographic algorithm storage section for storing a plurality of types of cryptographic algorithms decrypted by using a key for the encrypted algorithm~~[[,]]~~; and

said control ~~means~~ section, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructs said update cryptographic algorithm storage section, in place of said cryptographic algorithm storage section, to output the requested cryptographic algorithm as the information to be transmitted.

11. (Currently Amended) ~~[[An]]~~ The apparatus according to claim 9, further comprising a key ~~encrypt means~~ encryption section for, when the key for the encrypted algorithm is requested from said cryptographic communication terminal, encrypting the key for the encrypted algorithm to be transmitted, and inputting the encrypted key for the encrypted algorithm, as the information to be transmitted, to said encryption/decryption ~~means~~ section.

12. (Currently Amended) ~~[[An]]~~ The apparatus according to claim 11, wherein said key encryption ~~means~~ section encrypts the key for the encrypted algorithm by using a key unique to a cryptographic communication terminal of the partner.

13. (Previously Presented) A cryptographic communication system comprising not less than two cryptographic communication terminals each defined in claim 22.

14-16. (Canceled)

17. (Currently Amended) ~~[[A]]~~ The storage according to claim 23, wherein:
said control ~~means~~ section further comprises a program for, when a transmission request for any of the cryptographic algorithms stored in said cryptographic algorithm storage ~~means~~ section is received, instructing said cryptographic algorithm storage ~~means~~ section to output the requested cryptographic algorithm~~[[,]]~~; and
said encryption/decryption ~~means~~ section further comprises a program for encrypting the requested cryptographic algorithm as the information to be transmitted.

18. (Currently Amended) A storage according to claim 23, further comprising a program for, when a key for the encrypted algorithm is requested from the partner, inputting the corresponding key for the encrypted algorithm, as the information to be transmitted to the partner, to said encryption/decryption ~~means~~ section.

19. (Currently Amended) A cryptographic communication center apparatus having said storage medium defined in claim 23, comprising:

an updated cryptographic algorithm storage ~~means~~ section for storing a plurality of types of cryptographic algorithms encrypted by the key for the encrypted algorithm;
and

means for, when the cryptographic algorithm decryption key is requested from the partner, inputting a corresponding key for the encrypted algorithm, as information to be transmitted to the partner, to said encryption/decryption ~~means~~ section,

wherein said control ~~means~~ section stores a program for, when a cryptographic algorithm is requested from said cryptographic communication terminal, instructing said

update cryptographic algorithm storage means to output the requested cryptographic algorithm as the information to be transmitted.

20. (Currently Amended) [[A]] The system according to claim 13, wherein said cryptographic communication terminal acquires the cryptographic algorithm and a decryption key therefor from said cryptographic communication center apparatus.

21. (Currently Amended) [[A]] The system according to claim 11, wherein said cryptographic communication terminal acquires a cryptographic algorithm from another cryptographic communication terminal and acquires a corresponding decryption key from said cryptographic communication center apparatus.

22. (Currently Amended) A cryptographic communication terminal comprising:

a control section for designating an encrypted cryptographic algorithm and an encrypted encryption/decryption key to be used in the cryptographic communication based on identification information;

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication in encrypted form, and outputting ~~a designated~~ the encrypted cryptographic algorithm designated by the control section ~~, said cryptographic algorithm storage section storing an encrypted cryptographic algorithm;~~

~~cryptographic algorithm decryption means for decrypting the encrypted cryptographic algorithm;~~

~~a key information storage section for storing [[a]] and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm corresponding to the cryptographic algorithm, and outputting a designated key, said key information storage section storing a key for an encrypted algorithm used to decrypt an encrypted cryptographic algorithm as well as the key for cryptographic communication;~~

~~a key information decryption means section for decrypting an encrypted key from said key information storage section the encrypted encryption/decryption key used for cryptographic communication and the encrypted key used for decrypting the encrypted cryptographic algorithm to create an encryption/decryption key used for cryptographic communication and an decryption key for decrypting the encrypted cryptographic algorithm;~~

~~a cryptographic algorithm decryption section for decrypting the encrypted cryptographic algorithm to generate an cryptographic algorithm by using the decryption key for decrypting the encrypted cryptographic algorithm; and~~

~~control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which a cryptographic algorithm and key are to be used in the cryptographic communication; and~~

~~an encryption/decryption means section for decrypting received encryption information by using the cryptographic algorithm designated with respect to said~~

~~cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted~~
encrypting/decrypting communication messages by using the cryptographic algorithm and the encryption/decryption key used for cryptographic communication.

23. (Currently Amended) A computer readable medium storing a program for implementing:

a control section for designating an encrypted cryptographic algorithm and an encrypted encryption/decryption key to be used in the cryptographic communication based on identification information;

a cryptographic algorithm storage section for storing not less than one type of cryptographic algorithm used for cryptographic communication in encrypted form, and outputting a ~~designated~~ the encrypted cryptographic algorithm designated by the control section, said cryptographic algorithm storage section further comprising a program for ~~storing an encrypted cryptographic algorithm, and implementing cryptographic algorithm decryption means for decrypting the encrypted algorithm by using a key for the encrypted algorithm;~~

a key information storage section for storing ~~[[a]]~~ and outputting the encrypted encryption/decryption key designated by the control section to be used for cryptographic communication and an encrypted key used for decrypting the encrypted cryptographic algorithm corresponding to the cryptographic algorithm, and outputting a designated key;

~~control means for designating, with respect to said cryptographic algorithm storage section and said key information storage section, which cryptographic algorithm and key are to be used in the cryptographic communication; and~~

a key information decryption section for decrypting the encrypted encryption/decryption key used for cryptographic communication and the encrypted key used for decrypting the encrypted cryptographic algorithm to create an encryption/decryption key used for cryptographic communication and an decryption key for decrypting the encrypted cryptographic algorithm;

a cryptographic algorithm decryption section for decrypting the encrypted cryptographic algorithm to generate an cryptographic algorithm by using the decryption key for decrypting the encrypted cryptographic algorithm; and

an encryption/decryption means section for decrypting received encryption information by using the cryptographic algorithm designated with respect to said cryptographic algorithm storage section and the key designated with respect to said key information storage section, and encrypting information to be transmitted encrypting/decrypting communication messages by using the cryptographic algorithm and the encryption/decryption key used for cryptographic communication.

24. (New) The terminal according to claim 22, further comprising:
an ID storage section for storing the identification information.

25. (New) A cryptographic communication center apparatus for communicating with one or more cryptographic communication terminals, comprising:

a control section for determining a cryptographic algorithm, a decryption key for the cryptographic algorithm, and an encryption/decryption key for a cryptographic communication terminal to be used in the cryptographic communication based on identification information received from the cryptographic communication terminal;

a cryptographic algorithm storage section for storing one or more cryptographic algorithms used for cryptographic communication, and outputting the cryptographic algorithm determined by the control section;

a key information storage section for storing and outputting the encryption/decryption key used for cryptographic communication;

a terminal key information storage section for storing a plurality of encryption keys and outputting an encryption key specific to the cryptographic terminal;

an algorithm decryption key storage section for storing a plurality of cryptographic algorithm decryption keys and outputting the decryption key for the cryptographic algorithm;

a key encryption section for encrypting the decryption key for the cryptographic algorithm using the encryption key specific to the cryptographic terminal; and

an encryption/decryption section for encrypting the cryptographic algorithm and the encrypted decryption key for the cryptographic algorithm and for encrypting/decrypting communication messages by using the cryptographic algorithm and the encryption/decryption key used for cryptographic communication.